ANÁLISIS ECONÓMICO DEL SECTOR

OBJETO: RENOVACIÓN DE LAS LICENCIAS "STANDARD PROTECTION" Y "ZERO-DAY PROTECTION" PARA EL FIREWALL SOPHOS XGS 2300, ASÍ COMO EL SOPORTE Y MANTENIMIENTO DEL MISMO, CON EL OBJETIVO DE MANTENER Y GARANTIZAR LA SEGURIDAD PERIMETRAL DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA SEDE ADMINISTRATIVA PRINCIPAL DEL FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA.

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia, en observancia a lo instituido en el artículo 2.2.1.1.1.6.1. Del Decreto 1082 de 2015, desarrolla el presente análisis del sector económico con el fin de obtener un marco de referencia uniforme que propugna por el cumplimiento de los objetivos de eficiencia, eficacia y economía del Sistema de Contratación Pública en Colombia.

En busca de una comprensión integral del sector asociado al objeto del proceso de contratación, abordamos diversas perspectivas: legal, comercial, financiera, organizacional, técnica y de análisis de riesgo. Este enfoque multidimensional permite contextualizar el proceso dentro de un espectro amplio, considerando tanto las implicaciones normativas como las prácticas comerciales y financieras relevantes.

En el análisis se revela que las personas naturales y jurídicas aptas para ofrecer los bienes y/o servicios identificados en el estudio pertenecen a diferentes sectores de la economía. Los macro receptores, clasificados como primario o agropecuario, secundario o industrial (productores de bienes tangibles), por lo cual son considerados como sectores productivos y el terciario o de servicios (considerado no productivo), puesto que no produce bienes tangibles, pero contribuye a la formación del ingreso nacional y del producto nacional.

Es importante Resaltar que las actividades económicas se diferencian aún más dependiendo de su especialización

La estructura del presente análisis del sector económico da seguimiento a las directrices que sobre el referente establece la Agencia Nacional para la Contratación Pública- Colombia Compra Eficiente.

INTRODUCCIÓN

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia se encuentra en la necesidad de fortalecer, renovar e incorporar tecnologías para asegurar la prestación de los servicios misionales y de apoyo a la gestión. Es así, como dentro del componente tecnológico de la entidad prestar un servicio óptimo y asegurar los activos de información de los usuarios, tanto internos como externos, así como de la infraestructura tecnológica del FPS, requiere la renovación de las licencias "Standard Protection" y "Zero-Day Protection" del firewall de nueva generación ya adquirido, debido a que estas licencias se vencerán el 14 de diciembre de 2024. La no renovación de estas licencias implicaría que el firewall no pueda cumplir con su función de proteger la red, exponiendo a la entidad a riesgos de seguridad y ciberataques que comprometerían la integridad y disponibilidad de la información institucional.

Además, el soporte y mantenimiento del firewall son esenciales para garantizar la continuidad operativa y la protección efectiva de los activos de información. Este soporte incluye actualizaciones de firmware, resolución de incidentes, y asistencia técnica que aseguran la defensa contra amenazas cibernéticas avanzadas.

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

ASPECTOS GENERALES DEL MERCADO

En la actualidad, la continua implementación de servicios en línea de la entidad, su demanda cada vez más creciente o acceso por parte de los ciudadanos y personas conectadas a Internet, así como también el gran número de usuarios internos que se encuentran conectados a través diferentes dispositivos de procesamiento de datos, demanda la urgente necesidad de mantener los esquemas y servicios de seguridad para los activos de información institucional, toda vez que a través de diferentes medios públicos o privados se masifican e incrementa los riesgos a los que están expuestos.

La transformación digital no se limita únicamente a proporcionar una mejor experiencia al cliente externo a través de los canales virtuales, una atención al cliente ágil e integrada con las redes sociales; sino que también hace necesario que el cliente o colaborador interno tenga unas condiciones adecuadas para que las herramientas digitales estén disponibles, en la totalidad del tiempo, garantizando con esto que la información cumpla con características de integridad, confidencialidad y disponibilidad.

En Colombia, la máxima autoridad en materia de tecnología es el Ministerio de tecnologías de la información, establecimiento público del orden nacional encargado de promover el acceso, uso efectivo y apropiación masivos de las TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el crecimiento sostenible del desarrollo del país.

La normatividad vigente que rige en Colombia los temas de firewall está contenida entre otras en las siguientes normas:

DIRECTIVA PRESIDENCIAL No. 03 del 2021: Dentro de la cual se imparten LINEAMIENTOS DE SEGURIDAD DIGITAL : Con el fin de fortalecer las capacidades y la funcionalidad de las entidades en términos de ciberseguridad y resiliencia corporativa, en concordancia con estas directrices, se hace hincapié en la importancia de Evitar la instalación de programas o extensiones de navegadores de fuentes desconocidas ya que estas pueden traer malware (software malintencionado) que puede afectar la integridad de los dispositivos y exponer la información sensible no solo propia, sino de las redes a las que se conectan.

Conpes 3995 de 2020: POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL, señala el objetivo de establecer medidas para desarrollar la confianza digital a través de la mejora en la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

RESOLUCIÓN 459 DE 2011: Por otra parte, debido al avance de la implementación de la Estrategia de Gobierno en Línea por parte de las entidades, los sitios web del Estado se han convertido en foco atractivo para ataques cibernéticos. En este sentido, la Intranet Gubernamental del Programa Agenda de Conectividad – Estrategia de Gobierno en línea brinda a los sitios web de las Entidades del Estado una infraestructura de seguridad unificada (Firewall, IPS, Antivirus, IDS, entre otros)

RESOLUCIÓN 1740 DE 2007, ART 2.4 SEGURIDAD EN LA RED: Los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red, y la integridad del servicio, para evitar la interceptación, interrupción, e interferencia del mismo. Para tal efecto, deberán informar en su página web sobre las acciones adoptadas en relación con el servicio prestado al usuario final tales como el uso de firewalls, filtros antivirus y la prevención de spam, phishing, malware, entre otras.

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

1.1. ASPECTOS HISTÓRICOS DE LOS FIREWALL

En los primeros días de la conectividad informática, la protección de redes era una preocupación mínima, dado que el acceso era limitado y la interconectividad entre sistemas era reducida. Con la expansión de la ARPANET, que eventualmente evolucionaría en Internet, surgió la necesidad de proteger las redes y los datos de accesos no autorizados.

Fue en los años 80 cuando los firewalls empezaron a tomar forma, con filtros básicos de paquetes que permitían o denegaban tráfico según reglas preestablecidas, basándose en el origen o destino del tráfico. Sin embargo, estos filtros no podían ver más allá de las capas de red y transporte del modelo OSI, por lo que su funcionalidad era limitada y no tenían la capacidad de detectar o bloquear ataques más avanzados.

Primera Generación: Filtrado de Paquetes (1988)

Los primeros firewalls de filtrado de paquetes trabajaban en la capa 3 del modelo OSI (capa de red) y usaban reglas sencillas para decidir si permitían o bloqueaban tráfico basado en direcciones IP, protocolos y puertos. Un claro ejemplo fue el sistema de filtrado de paquetes que desarrolló Digital Equipment Corporation (DEC) en 1988, el primer "firewall" de la historia. Aunque rudimentarios, estos filtros fueron la base para las siguientes generaciones de firewalls.

Segunda Generación: Firewalls de Circuito y Filtrado a Nivel de Sesión (1990)

En la década de los 90, los firewalls evolucionaron para incluir inspección de estado (stateful inspection), también conocida como filtrado a nivel de circuito. Esta tecnología permitía que el firewall no solo revisara el paquete aislado, sino que entendiera el contexto de una sesión completa, lo que le permitía determinar si un paquete pertenecía a una conexión legítima ya establecida. Esta característica mejoró significativamente la seguridad y redujo la vulnerabilidad a ataques más sofisticados.

Tercera Generación: Inspección Profunda de Paquetes (2000)

A medida que la conectividad a Internet aumentaba y la cantidad de amenazas también, se desarrolló la inspección profunda de paquetes (DPI, por sus siglas en inglés), que permitió a los firewalls analizar el contenido de los paquetes en niveles superiores, como las capas de aplicación. Esto permitió detectar amenazas en protocolos específicos (HTTP, FTP, DNS), mejorando la capacidad para identificar ataques como el malware y los ataques de inyección de código. Aquí nacen los firewalls perimetrales de aplicación (WAF), que se especializan en proteger aplicaciones web contra amenazas específicas.

2005: Firewalls UTM (Unified Threat Management)

Con la explosión de nuevas amenazas de seguridad, como spyware, spam, phishing y gusanos, surge el concepto de UTM, o administración unificada de amenazas. Los dispositivos UTM combinan las funciones de firewall, antivirus, prevención de intrusiones (IPS) y filtrado de contenidos en un solo dispositivo. Aunque ofrecían protección integral, estos dispositivos tendían a reducir el rendimiento de la red debido a la carga de trabajo adicional.

Cuarta Generación: NGFW y Firewalls Basados en Inteligencia Artificial (2010)

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

Con el incremento en ataques avanzados y específicos, los firewalls de próxima generación (NGFW, por sus siglas en inglés) empezaron a implementarse alrededor de 2010. Estos firewalls combinan DPI con funciones avanzadas como el control de aplicaciones, identificación de usuarios y prevención de intrusiones, todo en tiempo real. Además, con el crecimiento del machine learning y la inteligencia artificial, algunos NGFW comenzaron a incluir análisis de comportamiento para identificar patrones de ataques y tomar decisiones autónomas de bloqueo o permiso de tráfico.

Firewall en la Nube (Cloud Firewall)

La adopción de la nube trajo una nueva generación de firewalls conocidos como Cloud Firewalls o FWaaS (Firewall as a Service), que ofrecen protección en redes distribuidas y dinámicas como entornos de nube pública y privada. Estos firewalls permiten políticas de seguridad centralizadas y escalables en un entorno de nube, adaptándose a la virtualización y a la elasticidad de estos entornos, donde los recursos cambian constantemente.

Firewalls Basados en Inteligencia Artificial y Análisis Predictivo (2020 en adelante)

En los últimos años, con la proliferación de amenazas de día cero y ataques cada vez más complejos, los firewalls han comenzado a adoptar técnicas de inteligencia artificial y machine learning para una defensa proactiva. Este enfoque permite a los firewalls anticipar amenazas en función del análisis de patrones de tráfico, identificando amenazas potenciales antes de que ocurran. Con estos avances, los firewalls modernos se han convertido en herramientas de seguridad predictiva, que no solo bloquean ataques conocidos, sino que también previenen riesgos emergentes.

Actualmente, los firewalls perimetrales han avanzado significativamente respecto a sus versiones iniciales, adaptándose a un entorno donde los ataques pueden llegar en cualquier forma y desde cualquier lugar. Los firewalls siguen evolucionando, incorporando cada vez más tecnología de machine learning y respondiendo de forma automática y en tiempo real a amenazas complejas. Sin duda, el firewall perimetral continúa siendo un componente crucial de la defensa en ciberseguridad, y su evolución refleja la necesidad de adaptarse y adelantarse a un panorama de amenazas en constante cambio.

2. ASPECTOS TÉCNICOS Y COMERCIALES

2.1. CLASIFICACIÓN DE LOS BIENES Y SERVICIOS UNSPSC

De acuerdo al clasificador de bienes y servicios de Naciones unidas – UNSPSC, de la página web http://www.colombiacompra.gov.co/Clasificacion, los códigos contenidos que identifican el bien o servicio son los siguientes:

UNSPSC	Segmento	Familia	Clase	Producto
43222501	Difusión de tecnologías de la información y telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipos de seguridad	Equipos de seguridad de red cortafuegos (Firewall)
43222502	Difusión de tecnologías de la información y telecomunicaciones	Equipos o plataformas y accesorios de redes	Equipo de seguridad	Equipo de seguridad de redes VPN

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

		multimedia o de voz y datos		
43222503	Difusión de tecnologías de la información y telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipos de seguridad	Equipos de seguridad de evaluación de vulnerabilidad
26121616	Maquinaria y accesorios para generación y distribución de energía	Alambres, cables, arneses	Cables eléctricos y accesorios	Cable de telecomunicaciones
26121620	Maquinaria y accesorios para generación y distribución de energía	Alambres, cables, arneses	Cables eléctricos y accesorios	Cable para interconexiones
43223303	Difusión de tecnologías de la información y telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Dispositivos y equipos para instalación de conectividad de redes y Datacom	Cable de conexión de comunicaciones de datos
39121601	Componentes, accesorios y suministros de sistemas eléctricos e iluminación	Equipos, suministros y componentes eléctricos	Dispositivos y accesorios para la protección de circuitos	Breakers de circuito
43223310	Difusión de tecnologías de la información y telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Dispositivos y equipos para la instalación de conectividad de redes y Datacom	Conector de Fibra Óptica
43223326	Difusión de tecnologías de la información y telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Dispositivos de conexión de red	Cable de conexión de Fibra Óptica
43223328	Difusión de tecnologías de la información y telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Dispositivos y equipos para la instalación de conectividad de redes y Datacom	Panel de conexión de Fibra Óptica
43222612	Difusión de tecnologías de la información y telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipos de servicio de red	Interruptores de Red
43233201	Difusión de tecnologías de la información y telecomunicaciones	Software	Software de seguridad y protección	Software de servidor de autenticación
43233203	Difusión de tecnologías de la información y telecomunicaciones	Software	Software de seguridad y protección	Software de manejo de seguridad de red o de redes privadas virtuales VPN

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

43233204	Difusión de tecnologías de la información y telecomunicaciones	Software	Software de seguridad y protección	Software de equipos de seguridad de red o de redes privadas virtuales VPN
43233205	Difusión de tecnologías de la información y telecomunicaciones	Software	Software de seguridad y protección	Software de manejo de seguridad de transacciones y de protección contra virus
81111802	Servicios basados en ingeniería, investigación y tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes	Servicios de administración de la unidad central
81111809	Servicios basados en ingeniería, investigación y tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes	Servicio de instalación de sistemas
43232901	Difusión de tecnologías de la información y telecomunicaciones	Software	Software para trabajo en redes	Software de acceso
43232915	Difusión de tecnologías de la información y telecomunicaciones	Software	Software para interconectividad de redes	Software de interconectividad de plataformas
83112203	Servicios de comunicaciones	Redes	Servicios de conectividad	Servicios de red privada virtual (VPN)

2.2. ASPECTOS COMERCIALES

Los firewalls perimetrales, aunque cuentan con tecnologías avanzadas y múltiples funcionalidades, dependen de una renovación constante de sus licencias para asegurar que mantengan su nivel óptimo de seguridad. Sin estas licencias, las funcionalidades críticas de seguridad dejan de estar habilitadas, exponiendo a la red a riesgos significativos. En este sentido, es esencial considerar algunos puntos clave al momento de renovar la licencia de un firewall Sophos XGS4300.

Aspectos Importantes al Renovar la Licencia de un Firewall

Protección continua y actualizada: La renovación de la licencia asegura que el firewall Sophos XGS4300 pueda seguir recibiendo las últimas definiciones de amenazas y parches de seguridad. Sin esta renovación, el firewall perdería acceso a estas actualizaciones, quedando vulnerable frente a amenazas avanzadas, como el malware polimórfico y los ataques de día cero.

Mantenimiento y soporte técnico: Con una licencia renovada, se tiene acceso a soporte técnico especializado y actualizaciones de firmware y software, lo cual es esencial para resolver problemas de funcionamiento o incompatibilidades de manera oportuna. Sin el soporte de la licencia, estos servicios dejarían de estar disponibles.

Acceso a funcionalidades avanzadas y optimización del rendimiento: Las licencias renovadas de firewalls de próxima generación incluyen mejoras en rendimiento y nuevas funciones, como análisis predictivo con inteligencia artificial y respuesta a incidentes en tiempo real. Sin la licencia, estas funcionalidades avanzadas no estarían habilitadas.

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

Beneficios de Tener un Firewall Sophos XGS4300 con Licencia Activa

Contar con una licencia activa ofrece ventajas claras en cuanto a seguridad y control de la red:

Protección contra intrusiones externas: La licencia activa permite mantener los sistemas de prevención de intrusiones (IPS) y los filtros de aplicaciones, esenciales para evitar accesos no autorizados y defenderse contra amenazas avanzadas que un firewall sin licencia no puede bloquear.

Control del tráfico y gestión de la red: La licencia permite el uso de herramientas para el control de aplicaciones, filtrado web y segmentación de usuarios, manteniendo la red ordenada y controlada en cuanto a ancho de banda y seguridad de los datos.

Limitaciones de un Firewall Sin Licencia Renovada

Si no se renueva la licencia, el firewall pierde su funcionalidad de seguridad y protección contra amenazas, y varios servicios esenciales dejarán de funcionar:

Desactivación de actualizaciones: Sin licencia, el firewall no puede acceder a las actualizaciones de seguridad ni a las nuevas definiciones de amenazas, volviéndose obsoleto frente a nuevos tipos de malware, exploits y ataques de día cero.

Pérdida de soporte técnico y mantenimiento: Sin licencia, no se tiene acceso a soporte técnico, lo cual dificulta resolver problemas de funcionamiento y afectaría la respuesta ante incidentes críticos.

Inhabilitación de la protección avanzada: Los servicios de filtrado, análisis de tráfico en tiempo real y protección contra amenazas avanzadas se desactivan, dejando la red expuesta a aplicaciones no autorizadas y posibles intrusiones.

Tipos de Licencias para el Firewall Sophos XGS4300

Protección Avanzada (Enhanced Protection): Añade filtrado de contenido avanzado, detección de amenazas en tiempo real y acceso a bases de datos de inteligencia de amenazas, fundamentales para redes de tamaño medio y alta actividad.

Protección de Día Cero (Zero-Day Protection): La licencia más completa, diseñada para redes críticas, que incluye protección contra amenazas de día cero mediante análisis en sandbox e inteligencia artificial. Esta licencia es esencial para la seguridad frente a las amenazas emergentes más avanzadas.

3. ANÁLISIS DE LA OFERTA

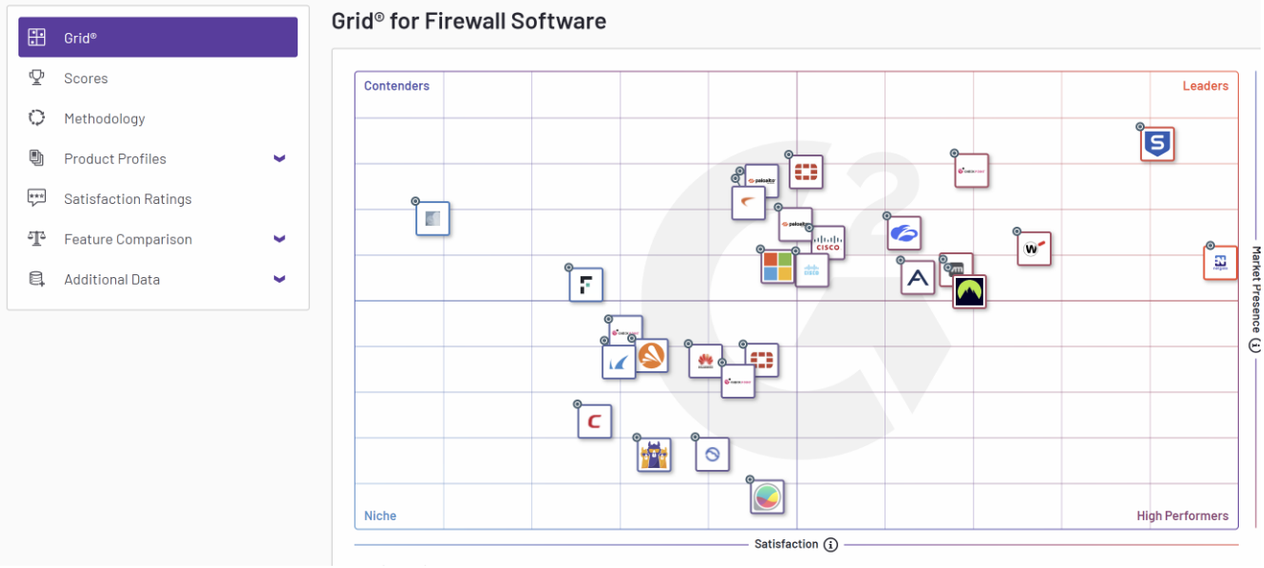
Colombia cuenta con un número significativo de empresas nacionales que han logrado acumular experiencia y conocimiento en la producción y prestación de servicios informáticos en diferentes sectores: entidades gubernamentales, comercio, industria manufacturera, transporte, almacenamiento, comunicaciones, electricidad, agua, gas, agricultura, caza, pesca[1].

[1] file:///C:/Users/TP/Downloads/Analisis%20del%20Sector%20Nube%20Privada%20Infraestructura%2016042020.pdf

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

Dentro de los servicios prestados en cuanto a la distribución de software licenciado hay decenas de firewalls, Que cumplen con los requerimientos y estándares más modernos en la lucha contra malwares, virus y demás amenazas; G2 es el mercado de software más grande y confiable. Más de un millón de personas al año, incluidos empleados de todas las empresas Fortune 500, utilizan G2 para tomar decisiones de software más inteligentes basadas en revisiones auténticas de pares.

Grid® Report for Firewall Software | Winter 2024



Leaders

	# of Reviews	Satisfaction	Market Presence	G2 Score
Sophos Firewall	207	91	92	92
Netgate pfSense	268	100	63	82
Check Point Next Generation Firewalls (NGFWs)	269	69	86	77
WatchGuard Network Security	203	77	67	72
Zscaler Internet Access	39	61	71	66
VMWare NSX	13	68	60	64
NordLayer	71	68	58	63
Arista NG Firewall	14	63	60	61
Cisco Secure Firewall Threat Defense Virtual (formerly NGFWv)	82	52	68	60

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

4. ESTUDIO DEL MERCADO

Sophos está catalogada dentro de los reportes de G2 como producto lider, obtenido una puntuación máxima de 92 puntos en cada una de las categorías presentadas por G2: satisfacción y presencia en el mercado. Esta calificación refleja la satisfaccion del producto en el usuario y su gran presencia en el mercado.

Teniendo en cuenta que el objeto contractual de este proceso es del fabricante SOPHOS, se procedió a realizar la verificación de los aliados estratégicos para la comercialización del producto en la página oficial del fabricante "https://partners.sophos.com/english/directory/search?country=Colombia" y se realizó la solicitud a través de correo electrónico de cotizaciones, recibiendo las siguientes propuestas:

ITSEC SAS

PRODUCTO	CANTIDAD	SUBTOTAL	IVA	VALOR TOTAL
RENOVACIÓN DE LAS LICENCIAS "STANDARD PROTECTION" Y "ZERO-DAY PROTECTION" PARA EL FIREWALL SOPHOS XGS 2300, ASÍ COMO EL SOPORTE Y MANTENIMIENTO DEL MISMO Por un periodo de 2 años	1	$ 39.018.672	$ 9.152.528	$ 48.171.200

SHCO Tech

PRODUCTO	CANTIDAD	SUBTOTAL	IVA	VALOR TOTAL
RENOVACIÓN DE LAS LICENCIAS "STANDARD PROTECTION" Y "ZERO-DAY PROTECTION" PARA EL FIREWALL SOPHOS XGS 2300, ASÍ COMO EL SOPORTE Y MANTENIMIENTO DEL MISMO Por un periodo de 2 años	1	$ 43.375.500	$ 10.174.500	$53.550.000

SIMYTEC

PRODUCTO	CANTIDAD	SUBTOTAL	IVA	VALOR TOTAL
RENOVACIÓN DE LAS LICENCIAS "STANDARD PROTECTION" Y "ZERO-DAY PROTECTION" PARA EL FIREWALL SOPHOS XGS 2300, ASÍ COMO EL SOPORTE Y MANTENIMIENTO DEL MISMO Por un periodo de 2 años	1	$ 49.045.500,00	$ 11.504.500	$ 60.550.000

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

En virtud de lo anterior, el Fondo ha determinado asignar como presupuesto base el promedio de las tres ofertas presentadas, la cual asciende a la suma de CINCUENTA Y CUATRO MILLONES NOVENTA MIL CUATROCIENTOS PESOS ($54.090.400) M/CTE.

5. ASPECTOS DE LA DEMANDA

5.1 CONTRATACIONES DE LAS ENTIDADES DEL SECTOR PÚBLICO

La demanda de servicios de firewall existe tanto en el sector público como en el sector privado, sin embargo, se ha revisado la demanda en el sector público debido a que es específicamente la relacionada con el objeto a contratar. Así, en el siguiente cuadro se detallan algunos procesos celebrados en el año 2024 en las entidades del estado.

ENTIDAD PÚBLICA	OBJETO CONTRACTUAL	MODALIDAD DE SELECCIÓN DEL CONTRATISTA	VALOR DE L CONTRATO	PLAZO DEL CONTRATO
MUNICIPIO DE PITALITO	RENOVACIÓN LICENCIAMIENTO SOPHOS PARA XGS 3300 POR 12 MESES XSTREAM PROTECTION XGS3300 EMAIL PROTECTION XGS3300 WEBSERVEPROTECTION	Mínima cuantía	44.999.850	30 DIAS
ESENTTIA S.A.	Renovacion de Cien (100) licencias: Kaspersky Endpoint Security for Business Select en la ultima version liberada por el fabricante, con soporte y mantenimiento por un (1) año..	Contratación régimen especia	168.998.360	365 DIAS

Los procesos contractuales que adelantan las entidades públicas para la contratación de servicios de firewall abarcan las modalidades de selección abreviada de mínima cuantía de modo que de acuerdo con el enfoque dado al objeto contractual la entidad determina la modalidad de selección a seguir para la escogencia del contratista.

5.2. CONTRATACIONES PREVIAS DEL FONDO

Dentro del Fondo Pasivo Social de Ferrocarriles Nacionales de Colombia se realizó la contratación que se menciona a continuación:

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

ENTIDAD	OBJETO CONTRACTUAL	MODALIDAD	VALOR
FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA	ADQUISICION DE LA LICENCIA DEL MOTOR DE BASE DE DATOS ORACLE STANDARD EDITION 2 PARA UN PROCESADOR POR TERMINO DE 2 AÑOS CON SOPORTE EN DESARROLLO DEL PROYECTO DE INVERSIÓN DENOMINADO "FORTALECIMIENTO DE LA GESTIÓN ADMINISTRATIVA, TECNOLÓGICA Y OPERATIVA DEL FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA, CÓDIGO BPIN NO. 2018011000373"	INVITACION PUBLICA DE MINIMA CUANTIA	$ 43,479,603
FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA	CONTRATAR LA ACTUALIZACIÓN DE 175 LICENCIAS DE SOFTWARE, EL SUMINISTRO E INSTALACIÓN Y CONFIGURACIÓN DE 100 NUEVAS LICENCIAS Y 275 LICENCIAS DE MESA DE AYUDA DEL SOFTWARE DE SEGURIDAD, LLAMADO PCSECURE. DESARROLLADO POR LA FIRMA TECNOLOGIA DE HARDWARE Y SOFTWARE PCTECHSOFT S.A.S. EN DESARROLLO DEL PROYECTO DE INVERSIÓN DENOMINADO "FORTALECIMIENTO DE LA GESTIÓN ADMINISTRATIVA, TECNOLÓGICA Y OPERATIVA DEL FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA, CÓDIGO BPIN NO. 2018011000373.	Contratación Directa (Ley 1150 de 2007)	$ 32,814,000

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

	FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA	ADQUISICIÓN DE TRESCIENTAS (300) LICENCIAS DE SOFTWARE DE ANTIVIRUS CON SOPORTE, GARANTÍAS Y PUESTA EN CORRECTO FUNCIONAMIENTO PARA USO EXCLUSIVO DEL FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA	Contratación Mínima Cuantía	$ 24,938,312	

ELABORÓ

ORTEGA MORAT NICOLAS

Firmado digitalmente por ORTEGA MORAT NICOLAS
Fecha: 2024.11.28 15:43:02 -05'00'

NICOLAS ORTEGA MORAT
JEFE OFICINA ASESORA PLANEACIÓN Y SISTEMAS

CARLOS ANDRÉS GRANADOS GUEVARA
CONTRATISTA OFICINA ASESORA PLANEACIÓN Y SISTEMAS

NOTA: La Oficina Asesora Jurídica contará con 5 días hábiles contados a partir de la fecha del recibido del presente documento para objetar, corregir, modificar o adicionar el contenido del presente escrito

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.

Este documento es propiedad de El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Prohibida su reproducción por cualquier medio, sin previa autorización.